

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 03-05-2010		2. REPORT TYPE FINAL		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE  Cyber Warfare as an Operational Fire				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)  Robert Majoris				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)  Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A: Approved for public release; Distribution is unlimited.					
13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy					
14. ABSTRACT  This paper explores cyber warfare as an option for creating operational fires effects. Initially, cyberspace is defined and explained from the perspective of the private sector. Following that, the paper describes the development of the military's current position on cyberspace. Then, operational fires are defined and the advantages of their use are explained. From there, discussion focuses on how cyber warfare fulfills the purposes of operational fires. Finally, the paper draws conclusions about the viability of cyber warfare as an operational fire and makes recommendations about how to prioritize the activities of the newly approved U.S. Cyber Command.					
15. SUBJECT TERMS Cyber, Cyber Warfare, Cyber warfare, Fire, Operational					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES  20	19a. NAME OF RESPONSIBLE PERSON Chairman, JMO Department
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code) 401-841-3414

**NAVAL WAR COLLEGE  
Newport, R.I.**

**Cyber Warfare as an Operational Fire**

**By**

**Robert Majoris**

**LCDR, USN**

**A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.**

**The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.**

**Signature: \_\_\_\_\_**

**03 April 2010**

## **Contents**

Introduction	1
Cyberspace	2
How the Military Views Cyberspace	2
Operational Fires	6
Discussion	7
Isolation	7
Preventing Enemy Supply And Sustainment	9
Neutralize Critical Enemy Functions or Facilities	11
Conclusions	13
Recommendations	14
Bibliography	16

## **Abstract**

### Cyber Warfare as an Operational Fire

This paper explores cyber warfare as an option for creating operational fires effects. Initially, cyberspace is defined and explained from the perspective of the private sector. Following that, the paper describes the development of the military's current position on cyberspace. Then, operational fires are defined and the advantages of their use are explained. From there, discussion focuses on how cyber warfare fulfills the purposes of operational fires. Finally, the paper draws conclusions about the viability of cyber warfare as an operational fire and makes recommendations about how to prioritize the activities of the newly approved U.S. Cyber Command.

## INTRODUCTION

In April 2007, the small and well networked country of Estonia sustained a crippling, week-long cyber attack affecting its economic and information infrastructures. Government websites, as well as banking, shopping and media portals were bombarded with false internet traffic originating from thousands of hijacked computers running 'bots'. This intense level of network activity created gridlock in the system servers.<sup>1</sup> Communication between the government and the people was disrupted. Worries about the status of financial accounts managed online caused panic. Most alarmingly, the cyber attack impacted the nation's leadership at the cognitive level, delaying a coordinated response. The responsible party successfully paralyzed the command and control functions of its target by using cyber warfare, highlighting an emerging set of war fighting capabilities. Computer network operations have come to represent a new and viable means of providing operational fires effects and are a force multiplier for the Joint Forces Commander. This paper will explore the argument presented. It will do so by offering a background of both cyber warfare and operational fires. Then, the paper will provide discussion of how cyber warfare fulfills the role of an operational fire. Examples will be given of recently conducted computer network attacks to help aid in the discussion. The paper will conclude by offering recommendations on a way forward as the United States continues to shape its cyberspace strategy.

---

<sup>1</sup> Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic" *Washington Post Foreign Service*, 19 May 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html> (accessed 30 April 2010).

## **CYBERSPACE**

Cyberspace was coined in 1982 by science fiction writer William Gibson in his story, “Burning Chrome.”<sup>2</sup> At the time, it had no real meaning outside of the story, but today cyberspace describes an official military domain along with land, sea, air, and space. What is cyberspace? Merriam-Webster’s online dictionary defines it as, “the online world of computer networks and especially the internet.”<sup>3</sup> When any networked user device sends or receives data, that data exists as binary code and travels temporarily through any of several different medium until it reaches its destination. At its destination the data is received and processed by another device. From point A to point B, a data stream may travel from an office network made of copper wire, to an internet service provider network made of fiber optic cable. From there, it may be sent via radio signal to a satellite and beamed across the ocean, where it may cross multiple additional networks before reaching its destination.

## **HOW THE MILITARY VIEWS CYBERSPACE**

It is understood that when conducting a major joint operation, planning efforts need to address the six operational functions. Joint Pub 3-0 lists these functions as Command and Control, Intelligence, Fires, Movement and Maneuver, Protection, and Sustainment. As written in Joint Pub 3-0, “[these] functions help JFCs to integrate, synchronize, and direct joint operations.”<sup>4</sup> As new technologies are incorporated into the military, these functions grow in depth and scope. For instance, with the advent of aviation in World War I, aerial surveillance was born. This new surveillance capability was categorized under the

---

<sup>2</sup> Gibson, William, *Burning Chrome* (New York: Arbor House, 1986), 179.

<sup>3</sup> *Merriam-Webster Online Dictionary*. s.v. “cyberspace.”, <http://www.merriam-webster.com/dictionary/cyberspace/> (accessed 20 April 2010).

<sup>4</sup> Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, final coordination, Joint Publication (JP) 3-0 (Washington DC: CJCS, 17 September 2006), xvi.

Intelligence function, broadening and improving the value of that category. Then, as aircraft technology matured, other capabilities emerged. It wasn't long before aircraft became an essential aspect of almost every military operation. Because of the development of this technology, all operational functions benefited. Ultimately, an entirely separate branch of the U.S. military was formed in 1947 with the inception of the Air Force.

Today's military is going through a similar transformation with the advent of the recently named cyberspace domain. The US military defines cyberspace as, "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."<sup>5</sup> This definition includes much more than just the Internet, as the military relies on networks that include satellites and proprietary networks that connect weapon systems.

Until 2005, when the United States Air Force added cyberspace to its mission statement, the U.S. Department of Defense maintained a very noncommittal attitude towards exploring the domain as a battle space. This is not to say that the military was slow to leverage cyberspace as a means to improve war fighting efficiency. In 1996, the Vice Chairman of the Joint Chiefs of Staff, Admiral William A. Owens, wrote an article published by The Strategic Forum titled, "The Emerging U.S. System-of-Systems."<sup>6</sup> This document laid out a revolutionary concept in which the military could leverage networks and computer technology to make combat power more precise and effective. The concept he described came to be known as network-centric warfare and is still being developed and used to shape U.S. military doctrine. Admiral Owens wrote briefly about the inherent risk of relying too

---

<sup>5</sup> Robert M. Gates, U. S. Secretary of Defense, *Quadrennial Roles and Missions Review Report*, January 2009, 15.

<sup>6</sup> William A. Owens, "The Emerging U.S. System of Systems," *The Strategic Forum* 63 (February 1996).

heavily on technology, but at no time did he conceive of a command dedicated to exploring these risks, either from an offensive or defensive standpoint.

This has not been the case worldwide. For the Chinese, the information warfare domain has been a focus area since the mid-1990s. As a way to offset the materiel disadvantages they faced with their out of date weapons, the Chinese considered cyber warfare an effective way to compete with modern, conventional military powers such as the United States. Michael Pillsbury, a research fellow at the National Defense University made this observation in 1997, “Judging by their military writings, they are saying that information warfare is the core of what they want to do. This way they can leap over the obsolescence of their tanks, ships, and aircraft and focus on the vulnerability of high-tech forces.”<sup>7</sup>

Realizations such as these forced the U.S. Department of Defense to take action. A Joint Task Force on Computer Network Defense was created in 1998. The task force was composed of 21 individuals and was charged with defending only Pentagon networks from cyber attack.<sup>8</sup> Space Command absorbed the task force the next fiscal year, and while the attempt did address the cyber realm, it did not treat it as a mature domain of war. The prevailing attitude towards cyber warfare could be seen in a comment made by Navy Captain Bob West, the deputy commander of the task force, in an interview with *Defense Daily*, “The odds of the U.S. being attacked online by a foreign nation state in some kind of cyber war in the near future are probably pretty low.”<sup>9</sup>

---

<sup>7</sup> Reuters, “Prelude to Infowar?,” June 24, 1998, <http://www.wired.com/news/politics/0,1283,13232,00.html> (accessed 20 April, 2010).

<sup>8</sup> Frank Wolfe, “Task Force Monitoring Cyber Intrusions Around Clock,” *Defense Daily* (July 27 1999), 1, <http://www.proquest.com/> (accessed April 12, 2010).

<sup>9</sup> Frank Wolfe, “Task Force Monitoring Cyber Intrusions Around Clock,” *Defense Daily* (July 27 1999), 1, <http://www.proquest.com/> (accessed April 12, 2010).

When the Air Force changed their mission statement to, “deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace,” the last word was received by the other branches with mixed approval.<sup>10</sup> Although the military had been quick to embrace the concept of network-centric warfare, it was unsure how to address the domain created by these same networks. It took four years of study and discussion before the nation came to understand that cyberspace was a domain that encompassed alluring capabilities, along with some severe vulnerabilities. In order to develop and secure the Defense Department’s presence in cyberspace, Secretary of Defense Robert Gates approved the establishment of the US Cyber Command in June, 2009. This sub-unified command will reside within the Strategic Command Functional Component Command.

Cyber Command will be responsible for offensive and defensive operations within cyberspace. As cyberspace is explored and developed, capabilities are emerging that will once again increase the breadth and scope of the joint operational functions. For instance, just as with early aviation, cyberspace can be used to collect intelligence. In fact, because cyberspace is designed to act as a conduit for information, it is ideally suited in this role. However, intelligence collection is only the most obvious use of cyberspace. Just as aircraft evolved to include command and control suites and electronic countermeasures, technologies are being created and tested in cyberspace that can be used to support major operations.

One compelling capability being explored is that of cyber attack. Joint Pub 3-0 labels one form of cyber attack as computer network attack and defines it as, “operations (to) disrupt, deny, degrade, or destroy information resident in computers and computer networks

---

<sup>10</sup> Anonymous, “Wynne Raises Cyber Battle Flag,” *Air Force Magazine*, (March 2010), 77, <http://www.proquest.com/> (accessed April 10, 2010).

(relying on the data stream to execute the attack), or the computers and networks themselves.”<sup>11</sup> The relevance of computer network attack is increasing by the day. Almost every conceivable adversary uses the networks that make up cyberspace. Whether those networks are used to make phone calls, establish internet contact with potential recruits, or control force tracking systems designed for command and control, cyberspace enables decision makers to conduct warfare more effectively and efficiently.

### **OPERATIONAL FIRES**

The argument that cyber warfare is a viable method of conducting operational fires requires a short treatment of this subject upon which the argument can be built. According to Milan Vego, “*Operational fires* can be described as the application of one’s lethal and/or nonlethal firepower for generating a decisive impact on the course and outcome of a campaign or major operation.”<sup>12</sup> Fires at an operational level are used to shape the area of operations by degrading the enemy’s ability to respond effectively when the main effort commences. Reducing the enemy’s ability to move or sustain troops from other parts of the theater is an example of an operational fire. Attacks beyond the area of operations that confuse or deceive the enemy over the location of the main assault are also example of operational fires.

Benefits derived from the employment of operational fires include the increased effectiveness of the forces assigned to the operation. If the enemy is denied access to supplies or reinforcements, then the attacking force is able focus its efforts more forcefully in the main sector, multiplying the effects. Another benefit of using operational fires is the

---

<sup>11</sup> Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, final coordination, Joint Publication (JP) 3-0 (Washington DC: CJCS, 17 September 2006), xvi.

<sup>12</sup> Milan N. Vego, *Joint Operational Warfare*. VIII-59.

psychological advantage created as the enemy analyzes confusing and contradicting information supplied by lethal or nonlethal operational fires. Operational fires can cause the enemy to mis-allocate forces based on erroneous information or contrived attacks.

## **DISCUSSION**

If cyber effects are to be considered operational fires, then they must be able to achieve the effects of operational fires. The following discussion will focus on three key purposes behind the use of operational fires and the relationship of cyber attack to achieving those purposes. These three are isolation of the area of operations, preventing enemy supply and sustainment, and neutralizing the enemy's critical functions and facilities.<sup>13</sup>

### **ISOLATION**

By using isolating effects beyond the operational area, the attacker reduces the enemy's ability to move forces into and out of the sector of main effort<sup>14</sup>. The result for the attacker is a battle problem in which the enemy's capabilities and force levels are better understood because they have been intentionally shaped.

Cyberspace is a domain that can be leveraged to support these types of shaping efforts. For instance, deployment of troops and equipment throughout the theater has become increasingly complex. To deal more efficiently with this complexity, deployment scheduling software and networked tracking tools are very commonly used to manage these tasks. These management systems are networked to allow for efficient data exchange between various necessary parties. They include everything from high level planning and

---

<sup>13</sup> Milan N. Vego, *Joint Operational Warfare*. VIII-63.

<sup>14</sup> Milan N. Vego, *Joint Operational Warfare*. VIII-63.

tracking software to train scheduling networks, air traffic control systems, or shipping inventory management tools. The same features that allow the system to provide quick, streamlined planning and execution also create vulnerabilities that can be exploited by cyber warfare. An intense cyber attack targeting deployment management networks could have effects ranging from system unavailability to data exploitation to intelligence collection.

In the first case, if cyber attacks denied the enemy access to his complex computer based deployment plan, deployment delays would occur. The enemy would be forced to adapt and reorganize. This could be a potentially lengthy process which would affect factor time. For the attacker, the advantage gained in time would be used to initiate operations in the now isolated sector of main effort. Operational success would now be more likely because the attacking military would be facing something less than the enemy's full combat power.

If data exploitation efforts were successful, then the enemy would be dealing with a system that was consistently deviating from the expected results.<sup>15</sup> An example would be a planning program that consistently reorganizes forces resulting in an unusable matching of troops to equipment. Program accuracy would be called into question and delays would again be imposed as efforts were made to correct the exploited system or transition to a new, reliable solution. For an attacker, the same benefits derived from a system denial would be enjoyed here, with the possible added benefit of creating a general climate of technological mistrust among the enemy. This may to some degree convince the enemy to give up the benefits of networked systems, slowing the enemy down relative to the attacker throughout the operation or even over the course of a campaign.

---

<sup>15</sup> Martin C. Libicki, *Cyberdeterrence and Cyber War*, RAND report (Santa Monica, CA: RAND, 2009), 57, 92.

In the final case, infiltration of the enemy's transportation management networks may result in intelligence detailing deployment plans including locations of embarkation, times of movements, etc. This information could be directed to a targeting cell for kinetic attack. By leveraging multiple domains, a Joint Force Commander can make his force more lethal and effective. In all cases, the fire effect of isolating the battlefield is achievable by leveraging cyberspace for attack and exploitation.

### **PREVENTING ENEMY SUPPLY AND SUSTAINMENT**

Related closely to the effect of isolation is the effect of denying the enemy logistical support and sustainment.<sup>16</sup> Whether at the logistics centers or while en-route, operational fires seek to disrupt enemy efforts to support and sustain their forces in the area of operations. This shaping effort can advance the enemy's culmination point in the sector of main effort, leading to a higher chance of success for the Joint Forces Commander.

Cyberspace lends itself to these effects as technological advances have been made to help streamline the logistics process. The transportation systems described in the last section support the logistics efforts of modern militaries. Therefore, attacks on these systems, similar to what was previously discussed, would have similar operational fires effects. Additionally, inventories and ordering systems are becoming increasingly dependent upon computer systems and the internet.<sup>17</sup> Military financial accounting systems share information across networks and keep data on computer systems in complex databases.<sup>18</sup> By affecting

---

<sup>16</sup> Milan N. Vego, *Joint Operational Warfare*. VIII-63.

<sup>17</sup> R. Crum, "Got Stuff? Logistics Modernization Gears Up To Deliver Faster and Better," *Leatherneck*, (September 2010), 52-56, <http://www.proquest.com/> (accessed 30 April, 2010).

<sup>18</sup> Unisys Corporation, "Unisys Awarded an Estimated \$187 Million Contract to Manage and Upgrade ClearPath Mainframe Environment for U.S. Department of Defense," *Defense & Aerospace Business*, (17 February 2010), 28, <http://www.proquest.com/> (accessed April 30, 2010).

the use of either of these two systems, the logistical supply and sustainment of a force in the operational area can be significantly impacted.

First, consider a cyber attack that destroys or exploits a supply inventory. This inventory might be composed of hundreds of thousands of critical supply items used to support enemy forces throughout a theater of operations. If the inventory were completely deleted or corrupted, it would take a long time to rebuild. If the inventory were corrupted, it may take even longer for the enemy to realize that portions of the inventory are wrong. This delay could prove to be deadly for the forces defending in the sector of main effort. For the attacker, they gain the advantage of facing an enemy whose ability to defend is rapidly dwindling.

Next, imagine the effect cyber warfare could have on the military requisition process. Perhaps a cyber weapon could be deployed that intercepts all incoming supply requisitions and deletes or changes them, while making appearances to the submitting computer that everything has been transmitted successfully. This would lead to a disruption in logistics services until the cyber weapon was found and neutralized. In the meantime, defending forces would be faced with supply delays or shortages. Additionally, and temporarily, friction between requesting forces and logistics services would arise prior to the cyber weapon being discovered.

An additional capability that cyber warfare provides is the ability to attack enemy financial systems. Imagine if all enemy aviation squadrons found their budgets for fuel reduced to zero. Confusion would arise and increase as the realization set in that these fuel dollars were not moved to a different account somewhere in the world, but that they were

simply deleted.<sup>19</sup> The accounting method relied upon for these large sums of money simply failed. By affecting funding lines, the enemy would be forced to reconstitute what has been taken from him. This would take time as it would potentially involve a governmental investigation. In the interim, the enemy's ability to obtain logistical supplies such as ammunition, fuel, and parts would all be restricted. During the time of adjustment, an operation could commence and the attacking force could enjoy the benefits of facing an enemy who is working with a restricted resupply chain. Due to the low cost of deploying cyber weapons, there is no reason why the logistics inventory, requisition and financial systems could not all be attacked, either simultaneously or sequentially in order to achieve the maximum effect.<sup>20</sup>

### **NEUTRALIZE CRITICAL ENEMY FUNCTIONS OR FACILITIES**

Operational fires are also designed to destroy or neutralize the enemy's critical functions or facilities.<sup>21</sup> Whether through denying the enemy use of their infrastructure or ports or airfields or bases, this effect focuses on the enemy's ability to leverage his own critical functions. By denying this to the enemy, the Joint Force Commander gains the upper hand in capabilities and force ratios.

Cyber warfare has demonstrated the ability produce these effects at various times across the globe. In the spring of 2000, a disgruntled Australian engineer used a cyber attack to take control of sewage pump valves, which led to raw sewage being pumped into

---

<sup>19</sup> 60-Minutes, "Cyberwar: Sabotaging the System," <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml?tag=currentVideoInfo;segmentTitle> (accessed 10 Apr 2010).

<sup>20</sup> Martin C. Libicki, *Cyberdeterrence and Cyber War*, RAND report (Santa Monica, CA: RAND, 2009), 147.

<sup>21</sup> Milan N. Vego, *Joint Operational Warfare*. VIII-63.

waterways, parks and hotel grounds<sup>22</sup>. In 2005, a Brazilian city just north of Rio de Janeiro lost power when a malicious hacker disabled a control system at a power plant. Tens of thousands of people were affected. Again, in 2007, Brazil was attacked from cyberspace, leaving 3 million residents of Espirito Santo without electricity for two days<sup>23</sup>. In both of these instances, hackers targeted critical nodes in the municipal infrastructure, weakening each city's means of sustainment, communication and mobilization. Finally, in March, 2007, the United States Department of Homeland Defense conducted a research experiment, codenamed "Aurora", during which a staged cyber attack was able to physically destroy a multi-million dollar electric generator similar to those used on the U.S. power grid<sup>24</sup>. This demonstration proved that cyberspace is a domain that is able to cross over into the physical realm, producing mechanical effects.

Prior to the initiation of a major operation, cyber attacks could be used to destroy critical components of the enemy's infrastructure, leaving them without the means to power their systems, or perhaps draw water, pump oil, or use their telecommunications. While cyber warfare may not be able to destroy critical facilities such as naval ports or airfields, the disruption that it can cause to critical infrastructure components can serve as a key enabler to lethal, kinetic fires designed to destroy or neutralize these facilities. By combining the capabilities of cyber warfare and other lethal fires, effects can be achieved at a much lower operational cost.

---

<sup>22</sup> Marshall Abrams and Joe Weiss, *Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia*, NIST Case Study (Gaithersburg, MA: National Institute of Standards and Technology, 2008), 1.

<sup>23</sup> 60-Minutes, "Cyberwar: Sabotaging the System," <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml?tag=currentVideoInfo;segmentTitle> (accessed 10 Apr 2010).

<sup>24</sup> Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN.com*, 26 September 2007, <http://www.cnn.com/2007/US/09/26/power.at.risk/index.html>, (accessed 02 May 2010).

The argument may be made that cyber operations are not viable as operational fires because they are only effective against those adversaries who depend upon the networks of cyberspace to support their war efforts. Unlike other domains, such as air and sea, the cyber domain does not present vulnerabilities to an adversary who does not subscribe to its services.<sup>25</sup> While this may be a valid argument today, it is much less valid than it was ten years ago, and will continue to be less relevant as cyberspace continues to grow. For example, between 2000 and 2009, the populations of Africa as well as the Middle East increased internet usage by over %1500.<sup>26</sup> This increase indicates that the cyberspace domain is growing as it becomes more accessible and affordable. In addition to the growth of the Internet, the CIA World Fact book estimates that over four billion people worldwide use cellular phones.<sup>27</sup> Speed and accessibility are characteristics that appeal to military organizations who desire the ability to coordinate forces over long distances. Cyberspace is an important military domain now, and it will continue to gain importance as time progresses.

## CONCLUSION

In a world that continues to increase its reliance on the internet and related networks for dissemination of information, the cyber domain is ripe with opportunities to affect the area of operations as a fires function. The most devastating effect of cyber warfare when employed as an operational fire is that it slows down the enemy, affecting factor time. When

---

<sup>25</sup> Martin C. Libicki, *Cyberdeterrence and Cyber War*, RAND report (Santa Monica, CA: RAND, 2009), 139-158.

<sup>26</sup> Internet World Stats, "Internet Usage Statistics," <http://www.internetworldstats.com/stats.htm> (accessed 15 April, 2010).

<sup>27</sup> CIA World Factbook, "Country Comparisons - - Telephones – Mobile Cellular," <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2151rank.html> (accessed 15 April, 2010).

any system is found to be infiltrated, systemic doubt begins to take hold. In extreme cases, this doubt can lead the enemy to abandon certain useful technologies, forfeiting the efficiencies afforded by these systems. Even in the most subtle cases, cyber warfare can cause an adversary to pause and investigate, costing time.

## **RECOMMENDATIONS**

Much of the current discussion concerning cyberspace is centered on the concept of cyber defense. Doctrine and policy that establishes conditions for the employment of pre-emptive or aggressive cyber attack is lacking. However, as the speed, size, and complexity of cyberspace continues to increase, new and more lethal capabilities should be developed in order for U.S. forces to benefit from the shaping capabilities offered by cyber warfare. Additionally, identifying vulnerabilities within adversary networks should be an ongoing effort. In order to maintain a cyber force that is prepared to support operations at all times, knowledge is crucial. This requires a commitment by the Department of Defense. This commitment is currently demonstrated by the creation of the U.S. Cyber Command. As this command matures, it will help to shape the nation's ideas about how to maintain its security and protect its national interests.

Cyberspace is a domain that is ideally suited to the application of operational fires. The global nature of the domain allows military forces to readily access the desired depth of the theater and produce effects without having to penetrate the enemy's kinetic defenses. The speed at which cyber warfare can be conducted also enables it to be precisely synchronized in a larger, more complex operational plan.<sup>28</sup> The cost of employing cyber

---

<sup>28</sup> Martin C. Libicki, *Cyberdeterrence and Cyber War*, RAND report (Santa Monica, CA: RAND, 2009), 158.

weapons is low, both in blood and treasure, making even subtle effects seem attractive to the operational planner. To develop cyber warfare and promote it as a viable shaping tool for operations around the world is becoming more important every day.

## BIBLIOGRAPHY

- 60-Minutes. "Cyberwar: Sabotaging the System."  
<http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml?tag=currentVideoInfo;segmentTitle> (accessed 10 Apr 2010).
- Abrams, Marshall, and Joe Weiss. *Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australi*. NIST Case Study. Gaithersburg, MA: National Institute of Standards and Technology, 2008.
- Anonymous. "Wynne Raises Cyber Battle Flag." *Air Force Magazine*, (March 2010): 77.  
<http://www.proquest.com/> (accessed April 10, 2010).
- CIA World Factbook. "Country Comparisons - - Telephones – Mobile Cellular."  
<https://www.cia.gov/library/publications/the-world-factbook/rankorder/2151rank.html> (accessed 15 April, 2010).
- Crum, R. "Got Stuff? Logistics Modernization Gears Up To Deliver Faster and Better." *Leatherneck*. (September 2010): 52-56. <http://www.proquest.com/> (accessed 30 April, 2010).
- Finn, Peter. "Cyber Assaults on Estonia Typify a New Battle Tactic." *Washingtonpost.com*, 19 May 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html> (accessed 30 April 2010).
- Gibson, William. *Burning Chrome*. New York: Arbor House, 1986.
- Internet World Stats. "Internet Usage Statistics."  
<http://www.internetworldstats.com/stats.htm> (accessed 15 April, 2010).
- Libicki, Martin C. *Cyberdeterrence and Cyber War*. RAND report. Santa Monica, CA: RAND, 2009.
- Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." *CNN.com*, 26 September 2007.  
<http://www.cnn.com/2007/US/09/26/power.at.risk/index.html> (accessed 02 May 2010).
- Owens, William A. "The Emerging U.S. System of Systems." *The Strategic Forum* 63 (February 1996).

Robert M. Gates, U. S. Secretary of Defense. *Quadrennial Roles and Missions Review Report*. January 2009.

Reuters. "Prelude to Infowar?" June 24, 1998.  
<http://www.wired.com/news/politics/0,1283,13232,00.html> (accessed 20 April, 2010).

Unisys Corporation. "*Unisys Awarded an Estimated \$187 Million Contract to Manage and Upgrade ClearPath Mainframe Environment for U.S. Department of Defense.*"  
Defense & Aerospace Business. (17 February 2010): 28.  
<http://www.proquest.com/> (accessed April 30, 2010).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations*. Final coordination. Joint Publication (JP) 3-0. Washington DC: CJCS, 17 September 2006.

Vego, Milan N. *Joint Operational Warfare*.